© 2018 IJSRST | Volume 4 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Detection of Node Capture Attacks in Wireless Sensor Networks

[1]K. Ravikumar, [2]V. Manikandan

[1]Assistant Professor, Department of Computer Science, Tamil University, Tanjavurr, Tamil Nadu, India
[2]Research Scholar, Department of Computer Science, Tamil University, Tanjavurr, Tamil Nadu, India

ABSTRACT

Wireless Sensor Network is a gathering of sensors with incomplete resources that collaborate in order to achieve a shared goal. It is susceptible to node capture attacks because sensor nodes are deployed in unattended manner. Once opponent imprisonments sensor nodes, he can compromise that node and presentation various types of occurrences with those compromised nodes. The antagonist takes the secret keying possessions from a compromised node, generates a large number of attacker-controlled imitations that share the cooperated node's keying materials and ID, and then feasts these replicas throughout the system. Therefore, captivity node attacks are perilous and should be noticed that node to reduce the harm. Several replica node detection schemes have been proposed against these attacks in static instrument networks. These methods are worked only in static sensor network and hence do not work in mobile sensor networks. In this work, propose a fast and effective mobile replication node discovery scheme using event-based attack decomposition. It shows logically and through imitation experimentations that our scheme detects mobile imitations in an efficient and robust method at the cost of judicious expenses.

Keywords : Sequential Analysis, Replica Detection, Wireless Sensor Network, Event-Based Attack Decomposition

I. INTRODUCTION

Wireless communication is a submission of science and technology that has come to be vital for modern presence. In advance, Wireless sensor Network is used in Wireless communication for transporting the information. Wireless sensor Networks have recently gained much consideration in the sense that they can be deployed for many different types of missions. In particular, they are useful for the assignments that are problematic for humans to carry out. For example, they are suitable for sensing dangerous natural singularity such as volcano eruption, biohazard monitoring, and forest fire detection. In addition to these dangerous applications, sensor networks can also be deployed for battle field shadowing, border monitoring, nuclear and chemical attack discovery, intrusion discovery, flood detection, weather forecasting, traffic shadowing and patient attention.

To carry out a variety of assignments, (Jun-Won Ho[1]) the system operator deploys the base position and a set of small sensor strategies in the network field. Specifically, sensor plans form ad-hoc networks, collaborate with each other to sense the marvel associated with the allocated missions and then sends the physical data to the base station. The network operator attains the mission related information by analyzing the data composed at the base station. To help instrument nodes carry out the missions professionally and effectively, many investigators proposed a variety of the network service and communication procedures. Specifically, localization, coverage, compression and combination protocols have been proposed for the system services. Various system protocols from physical layer to conveyance

IJSRST1841294 | Received : 12 Feb 2018 | Accepted : 25 Feb 2018 | January-February-2018 [(4) 2: 1301-1305]

layer have been proposed for the announcement (J.-Y.L. Boudec [2]).

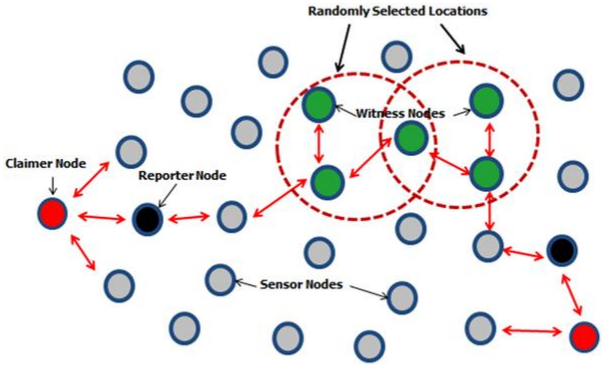

Figure 1. Sensor Network

A Wireless Sensor Network (WSN) is an assortment of sensors with limited possessions that collaborate in order to achieve a shared goal. Due to their functioning nature, WSNs are often unattended, hence prone to several kinds of novel attacks. For instance, an adversary could snoop on all network infrastructures and could capture nodes thereby obtaining all the information stored in database.
However, most of them focus on manufacture the protocols be attack-resilient rather than removing the source of attacks. Though attack-resiliency approach mitigates the threats on the network services and communication protocols, this method requires substantial time and effort to continuously enhance the sturdiness of the protocols in accordance with the appearance of new types of attacks. Moreover, since it is hard to forecast new types of attacks, the protocols will likely have resiliency only after being damaged by new types of occurrences. Thus, we need to detect and revoke the sources of attacks as soon as conceivable to considerably reduce the costs and damages incurred by employing attack-resilience approach. (S. Capkun[3])The principle sources of various attacks are compromised sensor nodes in the sense that assailant can compromise sensor nodes by exploiting the unattended countryside of wireless sensor systems and thus do any malicious activities with them (M. Conti[4]). To meet this need, recommend a node imprisonment attack detection scheme in wireless sensor networks. (K. Dantu [5]) It uses the fact that the actually captured nodes are not contemporary in the network during the period from the apprehended time to redeployed time. Subsequently, apprehended nodes would not contribute in any network processes during that period (J. Ho, M. Wright[6]).

II. LITERATURE SURVEY

A Randomized, Efficient, and Distributed (RED) protocol was future to enhance the line selected multicast scheme of in terms of copy detection probability, storage and calculation overheads (J. Ho, D. Liu[7]).

However, RED still has the same communication overhead as the line-selected multicast scheme. More significantly, their protocol requires repeated position claims over time, meaning that the cost of the scheme needs to be multiplied by the number of runs during the total deployment time. Contained multicast schemes based on the grid cell topology detect replicas by letting location claim be multicast to a single cell or manifold cells. The main strength of is that it achieves advanced detection rates than the best arrangement. However, has similar communication overheads as.

A clone discovery scheme was proposed in sensor systems (L. Hu and D. Evans [8]). In this scheme, the network is considered to be a set of non-overlapping sub counties. An exclusive subset is formed in each sub region. If the connection of subsets is not empty, it implies that replicas are included in those subsets. Fingerprint-based replica node discovery scheme was proposed in sensor networks(J.Jung,V. Paxon [9]). In this scheme, nodes report fingerprints, which classify a set of their neighbors, to the base station. The base station achieves replica detection by using the property that impressions of replicas battle each other

(K. Xing [10]).

III. PROBLEM DEFINITION

3.1 Network Models

Sensor systems are often deployed in an unattended manner, most of these protocols are exposed to a variety of attacks such as denial of facility attacks, routing disturbance and false data injection attacks, network service disturbance attacks. To defend the wireless sensor networks against these numerous attacks, many arrangements have been industrialized in the works. For instance, secure routing schemes have been proposed to alleviate routing disruption attacks. False data injection attacks can be alleviated by using the authentication schemes. Secure data combination protocols are used to stop attacker from disrupting combination. Many schemes have also been proposed to protect localization and time synchronization protocols from the threat.

It first assumes a static instrument network in which the positions of sensor nodes do not change after deployment. It also assumes that every instrument node works in promiscuous mode and is able to identify the sources of all messages originating from its neighbors. We believe that this assumption does not incur considerable overhead because each node inspects only the source IDs of the communications from its neighbors rather than the entire fillings of the messages.

3.2 Attacker Models

By assume that an attacker can physically capture sensor nodes to cooperation them. However, it places restrictions on the number of sensor nodes that he can physically capture in each target region. This is reasonable from the viewpoint that an increase in the number of the captured sensor nodes will lead to a rise in the probability that attacker is detected by intruder detection mechanisms. Therefore, a substance attacker will want to considerably capture the limited number of instrument nodes in each target region while not being detected by intruder detection mechanisms. Moreover, assume that it takes a certain quantity of time from taking nodes o redeploying them in the network. This is reasonable in the sense that an attacker needs some time to cooperation captured instrument nodes.

IV. PROPOSED SYSTEM

4.1 Node Capture Attack

In static sensor systems, a sensor node can be considered to be simulated if it is placed at more than one location. However, if nodes are allowed to freely roam through the network, the above method does not work because the mobile nodes location will unceasingly change as it moves. Hence, it is authoritative to use some other technique to detect imitation nodes in mobile sensor networks. Fortunately, movement provides us with a clue that can help resolution the mobile replica discovery problem. Specifically, a mobile sensor node should never move faster than the system-configured maximum speed. Consequently, if it notices that the mobile node "s speed is over the wide-ranging speed, it is then highly likely that at least two nodes with the same identity are present in the network.

To apply to the mobile replica detection problem as follows. Each period a moveable sensor node moves to a new position, each of its residents asks for a employed claim containing its location and time material and decides probabilistically whether to onward the conventional entitlement to the base station. The base position computes the speediness from every two uninterrupted claims of a mobile node and achieves the by taking speed as an experiential sample.

Each time highest speed is exceeded by the mobile node; it will accelerate the random walk to hit or cross the higher limit and thus lead to the base position accepting the alternative hypothesis that the moveable node has been simulated. On the other hand, each time the thoroughgoing speed of the mobile node is not reached, it will expedite the random walk to hit or cross the lower limit and thus principal to the base station tolerant the null hypothesis that mobile node has not been replicated. Once the base position decides that a mobile node has been replicated, it initiates cancelation on the replica nodes.

It also assumes that every moveable sensor node is able to obtain its location information and verify the locations of its neighboring nodes. This can be applied by employing GPS. This assumption may not lead to additional costs if the location material is used for other purposes. Finally, undertake that the clocks of all nodes are loosely coordinated with a thoroughgoing error of. This can be accomplished by the use of secure time.

4.2 Event-Based Attack Decomposition

It proposes a method for the expansion of suitable performance metrics for node capture attacks by decomposing the attack goal into a collection of events. By spacing the attack tasks into a graphical structure, the value of certain events can be computed via graph composition as a function of the corresponding sub-event values. Supposing that the adversary is interested in achieving a particular attack goal. This goal is most likely to cause some sort of noticeable effect on the network and it is likely to be an arrangement of a number of attack events. By disintegrating the goal into these separate events, the adversary is better able to gauge the progress of the attack toward the desired goal. To further simplify the attack evaluation, suggest a further rottenness of attack events into simpler subevents, until a collection of easily described primitive attack events is obtained, noting that such a decomposition need not be unique. The rottenness of the attack into these primitive events similarly allows for decomposition of the attack assessment metric into quantities that measure the value of achieving individual events. Once a set of nodes C has been captured, the attack presentation metric can be evaluated by recombining the values of the achieved primitive events by reversing the original putrefaction.

V. CONCLUSION

It is showed the boundaries of the benefits that attacker can take from launching node capture attacks when our scheme is employed. It also systematically showed that our preparation detects node capture attacks with a few number of samples while supporting the false positive and false negative rates below 1%. It is deliberated the ability to smash the goal of a node capture attack into primitive attack events and use the event-based putrefaction to evaluate the impact of an attack with admiration to the attack primitives. It illustrated the use of the event-based rottenness with an example node capture attack. Finally, decorated the potential for future research in the documentation of primitive attack events with respect to node imprisonment attacks in sensor systems.

VI. REFERENCES

[1]. Jun-Won Ho, Mathew Wright and Sajal K.Das (2011), "Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks using Sequential Hypothesis Testing‶, IEEE Transactions on Mobile computing.

[2]. J.-Y.L. Boudec and M. Vojnovi_c, "Perfect Simulation and Stationary of a Class of Mobility Models," Proc. IEEE INFOCOM,pp. 2743-2754, Mar. 2005.pp. 2743-2754, Mar. 2005.

[3]. S. Capkun and J.P. Hubaux, "Secure ositioning in Wireless Networks," IEEE J. Selected Areas in Comm., vol. 24, no. , pp. 221-232, Feb. 2006.

[4]. M. Conti, R.D. Pietro, L.V. Mancini, and A. Mei, "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication

Attacks in Wireless Sensor Networks," Proc. ACM MobiHoc, pp. 80-89, Sept. 2007.

[5]. K. Dantu, M. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G.S.Sukhatme, "Robomote: Enabling Mobility in Sensor Networks,"Proc. Fourth IEEE Int"l Symp. Information Processing in Sensor Networks (IPSN), pp. 404-409, Apr. 2005.

[6]. J. Ho, M. Wright, and S.K. Das, "Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis,"Proc. IEEE INFOCOM, pp. 1773-1781, Apr. 2009.

[7]. J. Ho, D. Liu, M. Wright, and S.K. Das, "Distributed Detection of Replicas with Deployment Knowledge in Wireless Sensor Networks, "Ad Hoc Networks, vol. 7, no. 8, pp. 1476-1488, Nov. 2009.

[8]. L. Hu and D. Evans, "Localization for Mobile Sensor Networks,"Proc. ACM MobiCom, pp. 45-57, Sept. 2004.

[9]. J.Jung,V. Paxon, A.W. Berger,andH.Balakrishnan,"Fast Portscan Detection Using Sequential Hypothesis Testing," Proc.IEEE Symp. Security and Privacy, pp. 211-225, May 2004.

[10]. K. Xing, F. Liu, X. Cheng, and H.C. Du, "Real-Time Detection of Clone Attacks in Wireless Sensor Networks," Proc. IEEE Int"l on f. Distributed Computing Systems ICDCS), pp. 3-10, June 2008.